

AD-A143 085

AN EXHAUSTIVE ANALYSIS OF MULTIPLICATIVE CONGRUENTIAL
RANDOM NUMBER GENER..(U) NORTH CAROLINA UNIV AT CHAPEL
HILL CURRICULUM IN OPERATIONS R.. G S FISHMAN ET AL.

1/1

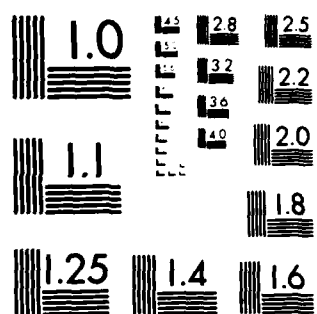
UNCLASSIFIED

JUN 84 UNC/ORSA/TR-84/5 N00014-76-C-0302

F/G 12/1

NL

END
DATE
FILMED
8-84
DTIC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

AD-A143 085

OPERATIONS RESEARCH AND SYSTEMS ANALYSIS

An Exhaustive Analysis of Multiplicative
Congruential Random Number Generators
with Modulus $2^{31}-1$

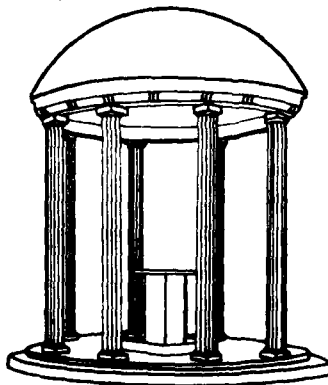
George S. Fishman^a

and

Louis R. Moore III^{a,b}

UNIVERSITY OF NORTH CAROLINA
AT CHAPEL HILL

DTIC FILE COPY



DTIC
ELECTE
JUL 11 1984
S B

DISTRIBUTION STATEMENT A

Approved for public release
Distribution Unlimited

84 07 10 198

An Exhaustive Analysis of Multiplicative
Congruential Random Number Generators
with Modulus $2^{31}-1$

George S. Fishman^a

and

Louis R. Moore III^{a,b}

Technical Report UNC/ORSA/TR-84/5

June 1984

^aCurriculum in Operations Research and
Systems Analysis

^bSchool of Business Administration

University of North Carolina at Chapel Hill

This research was supported by the Office
of Naval Research under contract
N00014-76-C-0302. Reproduction in whole or
part is permitted for any purpose of the United
States government.

DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

DTIC
ELECTE
S JUL 11 1984 D
B

An Exhaustive Analysis of Multiplicative
Congruential Random Number Generators
with Modulus $2^{31}-1$

George S. Fishman^a

and

Louis R. Moore III^{a,b}

Technical Report UNC/ORSA/TR-84/5

June 1984

^aCurriculum in Operations Research and
Systems Analysis

^bSchool of Business Administration

University of North Carolina at Chapel Hill

This research was supported by the Office
of Naval Research under contract
N00014-76-C-0302. Reproduction in whole or
part is permitted for any purpose of the United
States government.

DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

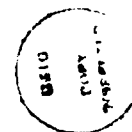
DTIC
ELECTE
JUL 11 1984
S D B

ABSTRACT

This paper presents the results of an exhaustive search to find optimal full period multipliers for the multiplicative congruential random number generator with prime modulus $2^{31}-1$. Here a multiplier is said to be optimal if the distance between adjacent parallel hyperplanes on which k-tuples lie does not exceed the minimal achievable distance by more than 25 percent for $k=2, \dots, 6$. This criterion is considerably more stringent than prevailing standards of acceptability and leads to a total of only 414 multipliers among the more than 534 million candidate multipliers.

Section 1 reviews the basic properties of linear congruential generators and Section 2 describes worst case performance measures. These include the maximal distance between adjacent parallel hyperplanes, the minimal number of parallel hyperplanes, the minimal distance between k-tuples, the lattice ratio and the discrepancy. Section 3 presents the five best multipliers and compares their performances with those of three commonly employed multipliers for all measures but the lattice test. Comparisons using packing measures in the space of k-tuples and in the dual space are also made. Section 4 presents the results of applying a battery of statistical tests to the best five to detect local departures from randomness. None were found. The Appendix contains a list of all optimal multipliers.

Key words: Congruential generator, discrepancy, lattice test, random number generation, spectral test.



For	
I	<input checked="" type="checkbox"/>
d	<input type="checkbox"/>
ion	<input type="checkbox"/>
on/	
ity Codes	
and/or	
cial	

A-1

INTRODUCTION

This paper presents the results of an exhaustive search to find optimal multipliers A for the multiplicative congruential random number generator $Z_i \equiv A Z_{i-1} \pmod{M}$ with prime modulus $M = 2^{31} - 1$. Since Marsaglia (1968) showed that k -tuples from this and the more general class of linear congruential generators lie on sets of parallel hyperplanes it has become common practice to evaluate multipliers in terms of their induced hyperplane structures. This study continues the practice and regards a multiplier as optimal if for $k = 2, \dots, 6$ and each set of parallel hyperplanes the Euclidean distance between adjacent hyperplanes does not exceed the minimal achievable distance by more than 25 percent. The concept of using this distance measure to evaluate multipliers originated in the spectral test of Coveyou and MacPherson (1967) and has been used notably by Knuth (1981). However, the criterion of optimality defined here is considerably more stringent than the criteria that these writers proposed. In fact, among the more than 534 million full period multipliers A examined in this study, our search identified only 414 optimal multipliers.

First proposed by Lehmer (1951), the multiplicative congruential random number generator has come to be the most commonly employed mechanism for generating random numbers. Jansson (1966) collected the then known properties of these generators. Shortly thereafter Marsaglia (1968) showed that all such generators share

a common theoretical flaw and Coveyou and MacPherson (1967), Beyer, Roof and Williamson (1971), Marsaglia (1972) and Smith (1971) proposed alternative procedures for rating the seriousness of this flaw for individual multipliers. Later Niederreiter (1976, 1977, 1978a,b) proposed a rating system based on the concept of discrepancy, a measure of error used in numerical integration. With regard to empirical evaluation, Fishman and Moore (1982) described a comprehensive battery of statistical tests and illustrated how they could be used to detect local departures from randomness in samples of moderate size taken from these generators.

Although the theoretical rating procedures have existed for some time, with the exception of Hoaglin (1976), Ahrens and Dieter (1977) and Knuth (1981), little use has been made of them. The present study, by its sheer exhaustiveness, removes this deficiency for generators with $M = 2^{31} - 1$. Section 1 reviews the basic properties of linear congruential generators. Then Section 2 describes the worst case performance measures that have been proposed to rate generators in k dimensions. These include the maximal distance between adjacent parallel hyperplanes, the minimal number of parallel hyperplanes, the minimal distance between k -tuples, the lattice ratio and the discrepancy. These concepts are described in this study principally in terms of the space of k -tuples and, where appropriate, in terms of the dual lattice space. However, in order not to obfuscate central concepts the exposition relies on a minimal use of formal lattice theory.

Section 3 presents the five best multipliers and compares their performances with those of three commonly employed multipliers for all these measures but the lattice test. The Appendix contains a list of all optimal multipliers. Also, lattice packing measures are presented and again show the dominance of the five best over the three commonly used multipliers. Packing measures in the dual space are also computed. This last concept is identical with Knuth's figure of merit for evaluating generators. Our results indicate that with regard to this criterion the five best perform better than all 30 multipliers listed in Table 1 of Knuth (1981, pp. 102-103). Bounds on discrepancy are also computed and discussed.

Section 4 presents the results of a comprehensive empirical analysis of the local sampling properties of the best five, using the procedures in Fishman and Moore (1982). No evidence of departures from randomness was detected.

1. Linear Congruential Generators

A linear congruential generator produces a sequence of non-negative integers

$$\{Z_0, Z_i \equiv AZ_{i-1} + C \pmod{M}; i=1,2,\dots\} \quad (1)$$

where the modulus M , and multiplier A are positive integers and the seed Z_0 and constant C are nonnegative integers. For purposes of conducting sampling experiments on a computer, the elements of the sequence Z are normalized to produce the sequence

$$U = \{U_i = Z_i/M; i=1,2,\dots\} \quad (2)$$

whose elements are treated as if they were sampled independently from the uniform distribution on the interval $[0,1)$. The objective in assigning values to M , A , Z_0 and C is to make the errors incurred in this treatment of U tolerable ones. Here errors are principally of two types, one being the approximation of a continuous phenomenon on $(0,1)$ by the discrete sequence U and the other being the distributional distortions in U induced by the use of the deterministic generator (1). In addition, computational considerations play a role in choosing M , A and C .

One property of the generator (1) is the period

$$T = \min \{k \geq 1: Z_{n+k} = Z_n \text{ for all } n \geq M\}. \quad (3)$$

The larger M is, the larger T can potentially be, and consequently the denser the points of U are in $[0,1)$. The more dense these points are, the smaller the continuity error is.

Table 1 lists several types of linear congruential generators that are or have been in common use. Here A , C , Z_0 in the table

Insert Table 1 about here

guarantee maximal period for the corresponding modulus M . Note that types 1 and 2 give full periods whereas the remaining generators give only one fourth of the numbers between 1 and 2^B . Moreover, types 4a and 4b do not produce equidistributed sequences. Also, the use of $M=2^B$ enables one to replace division and multiplication by less time consuming shift and add operations. Although $M=2^B-1$ does not allow this substitution

directly, a procedure due to Payne, Rabung and Bogyo (1969) enables one to retain part of this improved efficiency. Note that A is a primitive root of M if $A^{M-1} \equiv 1 \pmod{M}$ and $A^Q \not\equiv 1 \pmod{M}$ for $0 < Q < M-1$.

Today only linear congruential generators of types 2 and 3 are commonly used. On IBM computers with a word size of 32 bits and $C = 0$, the generator called SUPER-DUPER (Marsaglia 1972) uses $M = 2^{32}$, $A = 69069$ and $Z_0 = \text{odd integer}$ to give a period $T = 2^{30}$. For generators of type 2 with prime number modulus $M = 2^{31} - 1$, APL (Katzan 1971) uses $A = 16807$, the SIMSCRIPT II programming language (Kiviat, Villanueva and Markowitz 1969) uses $A = 630360016$, SAS (1982) uses $A = 397204094$ and the IMSL Library (1980) gives the user the choice of $A = 16807$ or $A = 397204094$. The resulting period is $T = 2^{31} - 2$.

2. Theoretical Measures Of Performance

In practice, it is relatively common to use the pseudorandom numbers produced by (1) in groups or k-tuples. Consider the sequence of points

$$W_k = \{W_{i,k} = (Z_{i+1}, \dots, Z_{i+k}); \quad i = 1, 2, \dots\} \quad (4)$$

and the normalized sequence

$$V_k = \{V_{i,k} = (Z_{i+1}/M, \dots, Z_{i+k}/M); \quad i = 1, 2, \dots\}. \quad (5)$$

Ideally one wants the sequence of points V_k to be equidistributed in the k -dimensional unit hypercube for $k = 2, 3, \dots$. However, the form of the generator (1) limits the extent to which

one can achieve this ideal. For example, observe that an ideal generator of the integers $1 \leq \{1, \dots, M-1\}$ produces $(M-1)^k$ equidistributed points in k -dimensional space whereas a generator of type 2 produces only $M-1$ points in this space.

Although this constancy of the number of points is itself sobering, it is one of two important issues. To illustrate the second issue, Fig. 1 shows a plot of 2-tuples for the generators $Z_i \equiv 7 Z_{i-1} \pmod{61}$ and $Z_i \equiv 31 Z_{i-1} \pmod{61}$ where 61 is a prime number and 7 and 31 are primitive roots of 61. Although no one would seriously use either of these generators to

Insert Fig. 1 about here.

produce random 2-tuples, a comparison of Figs. 1a and 1b arouses a concern that holds for more realistic generators as well. Notice that the distribution of points in Fig. 1b is considerably less uniform than the distribution in Fig. 1a. Since such differences in two and higher dimensions are attributable entirely to the choice of multiplier and since there are an enormous number of candidate multipliers, a deep analysis of k -tuples generated by (1) across all those multipliers is needed to assess the extent to which the resulting sequences V_k depart from the ideal of equidistributedness.

Several theoretical procedures have been proposed to make this assessment. They include:

1. maximal distance between adjacent parallel hyperplanes
(spectral test)

2. minimal number of parallel hyperplanes
3. minimal distance between points
4. ratio of lengths of longest and shortest minimal basis vectors (lattice test)
5. discrepancy.

Although diverse in what they measure, the procedures share a common unifying concept. All follow from recognizing that, with the exception of generators of types 4a and 4b, the k -tuples W_k can be regarded as points in a regular lattice. Moreover, generators of types 4a and 4b lead to k -tuples on two intermeshed regular lattices. Ahrens and Dieter (1977), Beyer, Roof and Williamson (1971) and Coveyou (1970) provide detailed descriptions of this relationship with lattice theory. To keep the focus of attention on the assessment of interest, the present paper presents only the features of lattice theory that are essential for describing these procedures. Also, unless otherwise noted our description applies for generators of type 2. Comparable analyses can be performed for each other type of generator.

2.1 Maximal Distance Between Adjacent Parallel Hyperplanes

Observe that Z_i can be written in the form

$$\begin{aligned}
 Z_i &\equiv Z_0 A^i \pmod{M} \\
 &= Z_0 A^i - M \sum_{m=0}^{i-1} K_{i-m} A^m \qquad i \geq 1
 \end{aligned}
 \tag{6}$$

where $K_j = \lfloor AZ_{j-1}/M \rfloor$ $j=1,2,\dots$. Now for $k \geq 1$, $\tilde{q} = (q_0, \dots, q_{k-1})$ and y consider the k -dimensional hyperplane

$$H_{\tilde{k}}(q, y) = \{(x_0, \dots, x_{k-1}) : \sum_{j=0}^{k-1} q_j x_j = y\}$$

and in particular the family of parallel hyperplanes

$$H_{\tilde{k}}(q) = \{H_{\tilde{k}}(q, y) : y \equiv 0 \pmod{1}\}. \quad (7)$$

Observe that the elements of V_k in (5) lie on hyperplanes in $H_{\tilde{k}}(q)$

in (7) if

$$(i) \quad q_0, \dots, q_{k-1} \text{ integer}$$

and

$$(ii) \quad q(A) = \sum_{j=0}^{k-1} q_j A^j \equiv 0 \pmod{M}.$$

These restrictions are sufficient since for any $V_{i,k}$ in V_k the quantity

$$y_i = \frac{1}{M} \sum_{j=0}^{k-1} q_j Z_{i+d}^j = \frac{Z_0 A^i}{M} q(A) + k_i \quad (8)$$

where

$$k_i = -\sum_{j=1}^{k-1} q_j \sum_{m=0}^{i+j-1} K_{i+j-m} A^m. \quad (9)$$

Restriction (i) insures that k_i is an integer and restriction (ii) insures that $y_i - k_i$ is an integer. These restrictions hold throughout the remainder of this paper.

For the ensuing analysis it is convenient to extend V_k modulo one to the set

$$V_k^* = \{V^* = (v_0^*, \dots, v_{k-1}^*) \text{ integer}\} \cup \{V^* = (v_0^*, \dots, v_{k-1}^*) \equiv V_{i,k} \pmod{1}; \\ i=1, \dots, T\}. \quad (10)$$

Since (i) and (ii) hold, the points in V_k^* also lie on hyperplanes in $H_k(q)$. The set of all hyperplanes containing at least one point of V_k^* is then

$$H_k^*(q) = \{H_k(q): y = \sum_{j=0}^{k-1} q_j v_j^*, \quad v^* \in V_k^*\}. \quad (11)$$

Moreover, one can index these hyperplanes by the set of integers

$$Y_k^*(q) = \{y^* = \sum_{j=0}^{k-1} q_j v_j^*: v^* \in V_k^*\}. \quad (12)$$

We now use these representations to show that for specified $k \geq 1$ and q the k -tuples in V_k lie on a set of parallel hyperplanes for which the Euclidean distance between adjacent hyperplanes is fixed. The set of hyperplanes is $H_k^*(q)$ and for y and z in $Y_k^*(q)$ the Euclidean distance between $H_k(q, y)$ and $H_k(q, z)$ is $|y-z| / (\sum_{j=0}^{k-1} q_j^2)^{1/2}$. To prove the result, it suffices to show that the $Y_k^*(q)$ is composed of all integer multiples of some fixed constant $I_k(q)$, for then the Euclidean distance between adjacent hyperplanes in $H_k^*(q)$ is

$$d_k(q; A, M) = \frac{I_k(q)}{(\sum_{j=0}^{k-1} q_j^2)^{1/2}}. \quad (13)$$

By way of proof, note that if V and V' are two elements of V_k^* then $V'' = V' - V$ is also $\in V_k^*$ therefore for y and z in $Y_k^*(q)$ one has

$y-z$ in $Y_{k\sim}^*(q)$. Also, for any integer j and point V^* in V_k^* the point $V' = jV^*$ is also in V_k^* so that $z=jy$, for $y \in Y_{k\sim}^*(q)$, is also in $Y_{k\sim}^*(q)$. Therefore, it follows that all elements of $Y_{k\sim}^*(q)$ are multiples of

$$I_{k\sim}^*(q) = \min\{|y^*| > 0; y^* \in Y_{k\sim}^*(q)\},$$

thus establishing (13). Without loss generality we take

$$(iii) I_{k\sim}^*(q) = 1.$$

Since many different vectors q satisfy (i), (ii), and (iii) for a given multiplier A and induce families of parallel hyperplanes, additional criteria are needed to enable one to characterize the extent of equidistributedness of the k -tuples V_k in (5) in the k -dimensional unit hypercube for each possible multiplier. One such criterion is the maximal distance between adjacent parallel hyperplanes which is a worst case measure for a particular multiplier A . It is

$$d_k^*(A, M) = \max_{q_0, \dots, q_{k-1}} \left[\left(\sum_{j=0}^{k-1} q_j^2 \right)^{-1/2} \right] \quad (14)$$

subject to restrictions (i), (ii) and (iii). In particular, note that the constraint (iii) eliminates the numerator of (13) from the maximization (14).

When using (14) to compare k -tuple performance for several multipliers for a type of generator, one prefers the multiplier

that gives the minimal maximal distance since this implies smaller empty regions in the k-dimensional unit hypercube for this multiplier than for the other multipliers. However, there is a limit to how small this maximal distance can be; in particular, it is known that (Cassels 1959, p. 332)

$$M^{1/k} d_k^*(A, M) \geq \gamma_k = \begin{cases} (3/4)^{1/4} & k=2 \\ 2^{-1/6} & k=3 \\ 2^{-1/4} & k=4 \\ 2^{-3/10} & k=5 \\ (3/64)^{1/12} & k=6. \end{cases} \quad (15)$$

To illustrate the significance of these bounds, note that with the modulus $M = 2^{31} - 1$ one has

$$d_k^*(A, 2^{31} - 1) \geq \begin{cases} .2008 \times 10^{-4} & k=2 \\ .6905 \times 10^{-3} & k=3 \\ .3906 \times 10^{-2} & k=4 \\ .1105 \times 10^{-1} & k=5 \\ .2157 \times 10^{-1} & k=6, \end{cases}$$

indicating the relative coarseness of the grid of points in as few as four dimensions.

Using multivariable Fourier analysis, Coveyou and McPherson (1967) advocated using the minimized "wave number"

$$\left(\sum_{j=0}^{k-1} q_j^2 \right)^{1/2}$$

(s.t. q_0, \dots, q_{k-1} integer and $q(A) \equiv 0 \pmod{M}$) to determine the relative desirabilities of alternative multipliers, hence the name spectral test. Shortly thereafter, it became apparent (Coveyou 1970; Beyer, Roof and Williamson 1971) that one could

perform equivalent studies using (14) by viewing the k -tuples as being arranged on parallel hyperplanes and exploiting the mathematical properties of the so induced lattice structure. In fact, it turns out that the physical interpretation of results can be more easily understood in the space of W_k whereas the computational procedures are more easily understood by working in the dual space of q . We return to this issue in Section 3.

2.2 Minimal Number of Parallel Hyperplanes

A second measure of equidistributedness, suggested by Marsaglia (1968), is the number of parallel hyperplanes $N_k(q_0, \dots, q_{k-1}; A, M)$ on which all the k -tuples lie. If this number is small for a particular multiplier A , then this is an indication that there exist large regions in the k -dimensional unit hypercube that contain no k -tuples.

Observe that with restriction (iii) gives the upper bound

$$N_k(q_0, \dots, q_{k-1}, A, M) \leq \sum_{j=0}^{k-1} |q_j|. \quad (16)$$

Using the development in Dieter (1975), one also observes that

$$-\sum_{j=0}^{k-1} (q_j)^- < Y_i^- < \sum_{j=0}^{k-1} (q_j)^+ \quad i=1, \dots, T$$

where

$$x^- = \begin{cases} 0 & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

and

$$x^+ = \begin{cases} x & \text{if } x \geq 0 \\ 0 & \text{if } x < 0. \end{cases}$$

Because of the restrictions (i) through (iii) the number of distinct $Y_i \pmod{1}$ is precisely the number of parallel hyperplanes $N_k(q_0, \dots, q_{k-1}; A, M)$, then

$$N_k(q_0, \dots, q_{k-1}; A, M) = \sum_{j=0}^{k-1} (q_j)^- + \sum_{j=0}^{k-1} (q_j)^+ = \sum_{j=0}^{k-1} |q_j| - 1. \quad (17)$$

The -1 in (17) follows from the observation that Y_i takes on all integer values $1, \dots, N_R(q_0, \dots, q_{k-1}; A, M)$.

As before, there exist many vectors q that satisfy restrictions (i), (ii), and (iii). A worst case measure here is

$$N_k^*(A, M) = \min_q N_k(q_0, \dots, q_{k-1}; A, M) \quad (18)$$

subject to the four restrictions. When using this criterion to choose among several multipliers, one prefers the one that gives the maximal minimal $N_k(q_0, \dots, q_{k-1}; A, M)$. As in the case of distance between hyperplanes, an upper bound exists on $N_k^*(A, M)$, namely (Marsaglia 1968)

$$N_k^*(A, M) \leq (k!M)^{1/k} \quad k=1,2,\dots$$

In particular, for $M = 2^{31} - 1$ the bounds are

$$N_k^*(A, M) \leq \begin{cases} 65536 & k=2 \\ 2344 & k=3 \\ 476 & k=4 \\ 191 & k=5 \\ 107 & k=6. \end{cases}$$

Again, these bounds are limiting, and encourage one to search for multipliers that can come close to the bounds.

Knuth (1981, p. 92) points out that the ordering of several multipliers A_1, \dots, A_p according to the maximal distance measure

$d_k^*(A,M)$ may differ from the ordering established by the minimal number of parallel hyperplanes measure $N_k^*(A,M)$. In particular, he notes that $N_k^*(A,M)$ "is biased by how nearly the slope of the lines or hyperplanes matches the coordinate axes of the cube." That is, $N_k^*(A,M)$ may be relatively large when $d_k^*(A,M)$ is also relatively large. Since in this case one inclines to discount the multiplier because of sparseness indicated by $d_k^*(A,M)$, there is some justification for valuing $d_k^*(A,M)$ more highly than $N_k^*(A,M)$ as a measure of performance. Section 3 takes this into consideration when searching for optimal multipliers.

Although $d_k^*(A,M)$ provides a more definite evaluation of a multiplier than $N_k^*(A,M)$ does, the latter quantity has at least one readily appealing attribute that justifies its consideration. We illustrate this feature for the type 3 generator with $A=65539$ and $M=2^{31}$. This generator is known as RANDU and was a standard feature of the IBM Scientific Subroutine Library on 360/370 series computers for many years. Observe that $65539 = 2^{16} + 3$ so that

$$Z_{i+1} \equiv (2^{16} + 3)Z_i \pmod{2^{31}}$$

$$Z_{i+2} \equiv (6 \times 2^{16} + 9)Z_i \pmod{2^{31}}$$

$$Z_{i+2} \equiv 6Z_{i+1} - 9Z_i \pmod{2^{31}}$$

$$Z_{i+2} - 6Z_{i+1} + 9Z_i \equiv 0 \pmod{2^{31}}.$$

Moreover,

$$U_{i+2} - 6U_{i+1} + 9U_i \equiv 0 \pmod{1}$$

indicating that $N_3^*(65539, 2^{31}) \leq 16$, a devastating indictment

of RANDU in three dimensions. Therefore, the valuable feature of $N_k^*(A, M)$ is that it can on occasion identify a poor multiplier with relatively little computational effort.

2.3 Distance Between Points

Smith (1971) has suggested an alternative measure of equidistributedness based on the minimal distance between k-tuples

$$c_k^*(A, M) = \min_{\substack{1 \leq i, m \leq T \\ i \neq m}} \left[\frac{1}{M} \sum_{j=0}^{k-1} (Z_{i+j} - Z_{m+j})^2 \right]^{1/2} \quad (19)$$

Since the total number of points is fixed at T, the smaller $c_k^*(A, M)$ is for a given A, the larger the volume of space is in the k-dimensional hypercube that is devoid of points. Therefore, when comparing several multipliers in k dimensions one prefers the one that gives the maximal $c_k^*(A, M)$.

Whereas $d_k^*(A, M)$ measures distance between adjacent parallel hyperplanes, $c_k^*(A, M)$ measures distance between nearest points. An alternative, but equivalent interpretation is to view $1/c_k^*(A, M)$ as the maximal distance between adjacent parallel hyperplanes in the dual space of g . This observation enables one to establish the upper bounds for $c_k^*(A, M)$ $k=2, 3, \dots$ (Cassels 1959, p. 332):

$$c_k^*(A, M) \leq 1/\gamma_k M^{1/k} \quad (20)$$

where γ_k is defined in (15). This duality relationship also facilitates the computation of $c_k^*(a, M)$ using the algorithm in Dieter (1975).

2.4 Discrepancy

The concept of discrepancy originated in the study of how well equidistributed sequences perform in sampling procedures designed to approximate the volumes of regions in the k -dimensional unit hypercube and in numerical integration. Having recognized the relationship between this problem and that of measuring the performance of a random number generator, Niederreiter (1977) adapted the discrepancy measure to this latter problem and gave bounds for it.

Consider the sequence of k -tuples $\{W_{i,k}; i=1,\dots,T\}$ defined in (4). For $N=1,\dots,T$ discrepancy in k dimensions for a multiplier A and a modulus M is defined as

$$D_N^{(k)}(A,M) = \max_R \left| \frac{\text{number of } W_{1,k}, \dots, W_{N,k} \text{ in } R}{N} - \frac{\text{volume of } R}{M^k} \right| \quad (21)$$

where R ranges over all sets of points of the form $R =$

$\{(w_1, \dots, w_k) | \alpha_1 \leq w_1 < \beta_1, \dots, \alpha_k \leq w_k < \beta_k\}$. Here α_j and β_j are integers in the range $0 \leq \alpha_j < \beta_j < M$ for $1 \leq j \leq k$ so that the volume of R is

$$\prod_{j=1}^k (\beta_j - \alpha_j).$$

Niederreiter (1977, 1978a) gave upper and lower bounds for

$D_N^{(k)}(A,M)$ for generators of types 1, 2 and 3 for arbitrary

$N \leq T$. In particular, the upper bound for generators of type 2

is

$$D_N^{(k)}(A, M) \leq \frac{k}{M} + \frac{\min(N, (M-N)^{1/2})}{N} \sum_{\substack{q \pmod{M} \\ q(A) \equiv 0 \pmod{M}}}^* \frac{1}{r(q, M)}$$

$$+ \frac{\max(0, N - (M-N)^{1/2})}{N} \sum_{\substack{q \pmod{M} \\ q(A) \equiv 0 \pmod{M}}}^* \frac{1}{r(q, M)}$$

where the asterisk denotes exclusion of $q_0 = \dots = q_{k-1} = 0$,

$$r(q, M) = \sum_{j=0}^{k-1} r(q_j, M),$$

$$r(q, M) = 1 \quad \text{if } q \equiv 0 \pmod{M}$$

$$= M \sin \pi \|q/M\| \quad \text{if } q \not\equiv 0 \pmod{M}$$

and

$$\|t\| = \min(t, 1-t).$$

Note that this bound holds for any local sample of N successive k -tuples from the generator as well as for a global evaluation of performance when $N=T$.

At present there exists no algorithm, other than total enumeration, for computing this upper bound and this situation is likely to remain so. However, the form of the bound enables one to establish a valuable relationship between the spectral test and discrepancy. Note that $\sin \|q/M\| > 0$ in the bound and that the number of such terms is a function of $q(A)$. Recall that the quantity

$$\left(\sum_{j=0}^{k-1} q_j^2 \right)^{1/2}$$

is minimized, subject to $q(A) \equiv 0 \pmod{M}$, to find the maximal distance between adjacent parallel hyperplanes. If this minimized quantity turns out to be small for a multiplier A , then the congruence occurs frequently for $0 \leq |q_{j-1}| < M$ $j=1, \dots, k$. This clearly adds positive terms to the second summation and therefore the upper bound is large. If for an alternative multiplier A' the minimized quantity turns out large, the congruence holds less frequently and the upper bound is smaller than in the previous case. Thus the results for the spectral test convey useful information about the bounds on discrepancy.

For generators of types 1 and 2, Niederreiter (1976, 1978a) also gave the lower bound

$$D_T^{(k)}(A, M) \geq \begin{cases} 1/k^k \rho^{(k)}(A, M) & \text{for } 2 \leq k \leq 6 \\ \pi/2(2\pi + 1)^k \rho^{(k)}(A, M) & \text{for } k \geq 7 \end{cases} \quad (22)$$

and the upper bound

$$\begin{aligned} D_T^{(k)}(A, M) &< \frac{k}{M} + \min(1, \frac{\sqrt{M-T}}{T}) (\frac{2}{\pi} \log M + \frac{7}{5})^k \\ &+ (\log 2)^{1-k} ((2 \log M)^k + 4 (2 \log M)^{k-1}) / 2 \rho^{(k)}(A, M) \\ &+ 2^k (2^{k-2} - 1) \binom{J+k-2}{k-1} / \rho^{(k)}(A, M) \end{aligned} \quad (23)$$

where

$$\begin{aligned} \rho^{(k)}(A, M) = & \min_{\substack{q \pmod{M} \\ \tilde{q} \neq (0, \dots, 0) \\ q(A) \equiv 0 \pmod{M}}} \prod_{j=0}^{k-1} \max(1, |q_j|) \quad (24) \end{aligned}$$

and

$$J = (\log M) / \log 2$$

Comparable results exist for generators of type 3.

With the exception of $k=2$ no algorithm exists for computing $\rho^{(k)}(A, M)$. Ahrens and Dieter (1977, Theorem 5.17) gave the stronger lower bound

$$D_T^{(k)}(A, M) \geq 1 / \left[\min_{\substack{q \neq (0, \dots, 0) \\ q(A) \equiv 0 \pmod{M}}} \left(\lambda_m^{k-1} \prod_{i=0}^{k-1} |q_i| \right) \right] \quad (25)$$

where m denotes the number of non zero q_i ,

$$\lambda_m = \begin{cases} m^m & \text{if } m = 2 \text{ or } 3 \\ m^m / (m-1)^m H_m & \text{if } m \geq 4 \end{cases} \quad (26)$$

and

$$H_m = \left[\sum_{j=0}^{\lfloor m/2 \rfloor + 1} (-1)^j \binom{m}{j} (\lfloor m/2 \rfloor + 1 - j)^{m-1} / (m-1)! \right]^m.$$

For $k=2$ Borosh and Niederreiter (1983) showed that

$$\rho^{(2)}(A, M) = \min_{0 \leq |q_1| \leq M/2} (|q_1| \cdot |tM - q_1 A|) \quad (27)$$

for some t satisfying $q_0 = tM - q_1 A$. This result makes the bounds in (22) and (23) operative for $k=2$.

Niederreiter (1977, 1978b) provided additional bounds for $k=2$. For type 2 generators

$$D_T^{(2)}(A, M) \leq (2 + \sum_{i=1}^p a_i) / T \quad (28)$$

and

$$D_T^{(2)}(A, M) \leq [2 + C(K) \log T] / T \quad (29)$$

where a_1, \dots, a_p are the partial quotients in the continued fraction expansion of A/M , $K = \max(a_1, \dots, a_p)$ and $C(K) = 2/\log 2$ for $1 \leq K \leq 3$ and $C(K) = (K+1)/\log(K+1)$ for $K \geq 4$. Expressions (28) and (29) also hold for type 3 generators with $2/T$ replaced by $1/T$ and with a_1, \dots, a_p being the partial quotients of $A/2^{B-2}$. Earlier, Dieter (1971) derived closely related results based on continued fractions to nearest integers rather than regular continued fractions.

Borosh and Niederreiter (1983, Table 2) have carried out a systematic search for multipliers of type 3 and type 4. In particular, they gave maximal period multipliers with $K \leq 3$ for $B = 6, 7, \dots, 35$ for each type.

2.5 Lattice Test

Beyer, Roof and Williamson (1971) and Marsaglia (1972) proposed an alternative figure of merit, for evaluating alternative multipliers, based on the concept of squareness. We use Fig. 1 to illustrate this concept. Clearly one can construct a vast number of parallelograms of varying areas that include no interior points. The presumption of the lattice test is that one prefers multipliers that produce parallelograms of minimal area whose sides are close, if not equal, in length; hence, the notion of squareness, where angles are neglected.

Now the minimal volume of a k -dimensional parallelepiped generated by k -tuples from (1) subject to (ii) is M^{k-1} . In evaluating a particular multiplier, the objective of the lattice test is to find the basis vectors $\alpha_1, \dots, \alpha_k$ that come closest

in k dimensions to achieving this squareness for parallelepipeds of volume M^{k-1} . To measure the extent of the departure from equidistributedness in k dimensions Beyer, et al. and Marsaglia recommended the quantity

$$R_k(A) = \frac{\max_{1 \leq i \leq k} |\alpha_i|}{\min_{1 \leq i \leq k} |\alpha_i|} ; \quad (30)$$

that is, the ratio of the lengths of the longest and the shortest basis vectors. Clearly $R_k(A) \geq 1$ and presumably one prefers multipliers for which $R_k(A)$ is close to unity.

It is worthwhile noting that the basis vectors $\alpha_1, \dots, \alpha_k$ play an implicit role in the previously mentioned tests as well. For example, one can show that for $k=2$ the maximal distance between parallel hyperplanes is

$$d_2^*(A, M) = (|\alpha_2|^2 - |\alpha_1 \cdot \alpha_2|^2 / |\alpha_1|^2)^{1/2}$$

where we take α_2 to be the longer vector.

Although the figure of merit in (30) has intuitive appeal, there is no universal agreement about its usefulness in identifying good multipliers. Marsaglia (1972, p. 275) suggested a generator of type 3 called super-duper with $M = 2^{32}$ and $A = 69069$.

It has $R_2(A) = 1.06$, $R_3(A) = 1.29$, $R_4(A) = 1.30$ and $R_5(A) = 1.25$; an appealing generator as evaluated by the lattice test. For this generator Niederreiter (1978, pp. 1027-1028) showed that $\rho^{(2)}(A, M) \leq 69069$ so that (22) gives $D_T^{(2)}(A, M) \geq 1/(4 \times 69069) = .3620 \times 10^{-5}$. But

Borosh and Niederreiter gave a multiplier $A = 30391/861$ for $M = 2^{32}$ with $\rho^{(2)}(A, M) = .2517M$ and $\sum_{i=1}^p a_i = 51$ for which (28) based on $M = 2^{32}$ gives $D_T^{(2)}(A, M) \leq (1 + 51)/2^{30} = .4843 \times 10^{-7}$. This result illustrates that although super-duper has the appealing figure of merit $R_2(69069) = 1.06$, there exist multipliers with $A \equiv 5 \pmod{2^{32}}$ that dominate it by a substantial margin in $k=2$ dimensions with regard to discrepancy.

3. Analysis

This section presents results of an investigation based on the evaluation of $\{d_k^*(A, M); k=2, \dots, 6\}$ for all multipliers A that are primitive roots of $M=2^{31}-1$, using an algorithm of Dieter (1975), as described in Knuth (1981, algorithm S). Hardy and Wright (1960) show that the number of primitive roots for M prime is $\phi(M-1)$ where

$\phi(M-1)$ = number of integers not exceeding and relatively prime to $M-1$.

This quantity is called the Euler totient function. Since $\phi(M-1)/(M-1) \doteq .249$ for $M=2^{31}-1$ (Ahrens and Dieter 1977, p. 7,6), one has $\phi(2^{31}-2) \doteq 534723428$, a not inconsequential number.

To find the primitive roots, one notes that if B is the smallest primitive root of the prime modulus M , then every primitive root has the form

$$A \equiv B^I \pmod{M}$$

where I is an integer whose largest common factor with $M-1$ is unity. Since one also can show that for every such I there exists a pair of multipliers $B^I \pmod{M}$ and $B^{M-1-I} \pmod{M}$ with identical lattice structures, it suffices to investigate only half of all the primitive roots. In the present case 7 is the smallest primitive root of $2^{31}-1$ so that only 267361714 multipliers require examination. Note that the multiplier with exponent $M-1-I$ produces the same sequence as the multiplier with exponent I does, but in reverse order.

Clearly one needs to adopt a screening procedure to identify and collect those multipliers that "perform well". For present purposes, the multipliers of most interest are those that "perform well" in $k=2, \dots, 6$ dimensions relative to the constraints imposed on all lattices in these dimensions. Consider the ratios

$$S_{1,k}(A,M) = \gamma_k / d_k^*(A,M) M^{1/k} \quad k=2, \dots, 6.$$

As seen from (15), $0 < S_{1,k}(A,M) \leq 1$. Now the closer $S_{1,1}(A,M), \dots, S_{1,6}(A,M)$ are to unity the better the performance is of this multiplier with regard to the achievable bounds in $2, \dots, 6$ dimensions. Therefore, one way to perform the screening is to identify all multipliers for which

$$\min_{2 \leq k \leq 6} S_{1,k}(A,M) \geq S \quad 0 < S < 1$$

where S is specified.

Initially we chose $S=.75$. Since preliminary computations indicated that there were an unmanageable number of multipliers that satisfied this criterion, we changed S to $.80$. This resulted in a total of 207 optimal multipliers, as listed in the

Appendix. Recall that there are actually twice this number of optimal multipliers. The abrupt reduction in the number of optimal multipliers when shifting from $S=.75$ to $S=.8$ is itself notable. Also note that any multiplier for which $S_{1,k}(A,M) > .8$ for $k=2, \dots, 6$ guarantees that for each k the distance between adjacent hyperplanes does not exceed the minimal achievable distance by more than 25 percent.

For each selected multiplier and $k=2, \dots, 6$ we also computed the ratios

$$S_{2,k}(A,M) = N_k^*(A,M)/(k!M)^k$$

and

$$S_{3,k}(A,M) = c_k^*(A,M)/\gamma_k M^{1/k},$$

again using Dieter's algorithm.

Table 2 presents these ratios for the multipliers with the five largest $\min S_{1,k}(A,M)$. It also presents results for $A=16807$ which is in APL and IMSL, for $A=397204094$ which is in IMSL and SAS, for $A=630360016$ which is the SIMSCRIPT 11 multiplier, and for $A=7$. This last multiplier illustrates the contrasts that are possible in performance.

Table 2 allows one to make several notable observations:

Insert Table 2 about here.

- (a) The first five multipliers perform considerably better than the remaining multipliers in the table with regard to the screening measures $\{S_{1,k}(A,M)\}$ and with regard to $\{S_{2,k}(A,M)\}$ and $\{S_{3,k}(A,M)\}$.

- (b) For each of these five multipliers $S_{1,2}(A,M), \dots, S_{1,6}(A,M)$ are remarkably close.
- (c) The measures $S_{3,2}(A,M), \dots, S_{3,6}(A,M)$ are also remarkably close and behave essentially as $S_{1,2}(A,M), \dots, S_{1,6}(A,M)$. As expected, $S_{1,2}(A,M) = S_{3,2}(A,M)$.
- (d) $S_{2,2}(A,M), \dots, S_{2,6}(A,M)$ show considerably more variation; no doubt a reflection of the suboptimality of these multipliers with regard to this criterion.

We now turn to another method of evaluating performance which derives from the concept of packing a lattice with spheres (see Cassels 1959). Recall that $c_k^*(A,M)$ is the distance between nearest points in the unit hypercube of k -tuples. Then the volume of a sphere with this diameter is

$$L_k(A,M) = \frac{\pi^{k/2} (c_k^*(A,M)/2)^k}{\Gamma(k/2 + 1)}$$

where $\Gamma(\cdot)$ denotes the Gamma function. Suppose one packs the lattice with such spheres centered on each of the $M-1$ points V_k in (5) and at the origin. Note that these spheres merely touch and that since there are only M k -tuples, the proportion of the unit hypercube packed with these spheres is $ML_k(A,M)$.

Let

$$\omega_k(A,M) = 2^k ML_k(A,M).$$

Using the lattice packing constants in (15) and (20) one has

$\omega_k(A, M) \leq$	{	3.63	k=2
		5.92	k=3
		9.87	k=4
		14.89	k=5
		23.87	k=6

Table 3 lists $\omega_k(A, M)$ for the five best and the three other commonly employed multipliers. The benefits of the five multipliers is again apparent since their packings are considerably better across dimensions than those for the more commonly used multipliers.

Knuth (1981, p. 102) has also used this concept of packing to rate multipliers. However, his approach relates to packing spheres in the dual space of $q_0/M, \dots, q_{k-1}/M$. This is done by noting that in addition to $d_k^*(A, M)$ being the maximal distance between neighboring parallel hyperplanes in the space of V_k , the quantity $1/Md_k^*(A, M)$ is the minimal distance between points in the dual space of $q_0/M, \dots, q_{k-1}/M$. Therefore, the volume of a sphere with radius $1/2d_k^*(A, M)$ in the dual space is

$$W_k(A, M) = \frac{\pi^{k/2}}{\Gamma(k/2+1) [2Md_k^*(A, M)]^k}$$

Now observe that restrictions (i) and (ii) determine that the hypercube $[-1, 1]^k$ contains exactly $2^k M^{k-1}$ k -dimensional points q/M . In particular, the exponent $k-1$ instead of k on M is due to restriction (ii). Therefore, the proportion of this unit hypercube packed with spheres is

$$\mu_k = 2^k M^{k-1} W_k(A, M)$$

$$= \frac{\pi^{k/2}}{\Gamma(k/2 + 1) M(d_k^*(A, M))^k}$$

which is the measure of packing in the dual space. This quantity is identical with the figure of merit suggested by Knuth (1981, p. 101). Note that because of the lattice structure in the dual space every other unit hypercube in this space would lead to the same $W_k(A, M)$ and $\mu_k(A, M)$.

Table 4 lists $\mu_k(A, M)$ for the multipliers of interest. Again note the better performance of the top five. Knuth remarks that one might say that any multiplier for which $\mu_k(A, M) \geq .1$ $k=2, \dots, 6$ passes the spectral test and any multiplier for which $\mu_k(A, M) \geq 1$ $k=2, \dots, 6$ passes the test with flying colors. By this standard the top five multipliers are untouchable. In fact, since $S_{1,k}(A, M) \geq .8$ $k=2, \dots, 6$ for all multipliers in the Appendix, those multipliers have

$$\mu_k(A, M) \geq \left\{ \begin{array}{ll} 2.32 & k=2 \\ 3.03 & k=3 \\ 4.04 & k=4 \\ 4.88 & k=5 \\ 6.26 & k=6 \end{array} \right.$$

indicating that all meet the Knuth criterion and dominate all multipliers listed in Table 1 of Knuth (1981, pp. 102-103).

Table 5 presents bounds on discrepancy computed from (25) and (28) and reveals several interesting results. First, note that the intervals for $k=2$ can in no way be regarded as narrow.

Second, the top five multipliers do not dominate A=397204094 and 630360016 unambiguously, as in the earlier tables. This lack of discrimination on the part of the lower bounds on discrepancy may be due to the fact that discrepancy is not a rotation invariant measure. That is, it is developed along the lines of the classical serial test in Statistics in which the sides of the cells are parallel to the coordinate axes and hence discrepancy detects the worst case with regard to this orientation only. By contrast, $d_k^*(A,M)$ measures the worst case with regard to all possible orientations. Although one can argue that many statistical testing procedures rely exclusively on this cartesian product space specification, the fact that our study reveals so many multipliers that perform well on the more stringent measure $d_k^*(A,M)$ encourages us to recommend this criterion for general use.

As mentioned earlier the Appendix contains a list of all multipliers for which $\min_{2 \leq k \leq 6} S_{1,k}(A,M) \geq .80$. A perusal of this list reveals six multipliers for which $S_{3,k}(A,M) \geq .80$. While these multipliers do not rank as high as the five best with regard to $\min_{2 \leq k \leq 6} S_{1,k}(A,M)$, their relatively good bivariate behavior with regard to $S_{1,k}(A,M)$ and $S_{3,k}(A,M)$ encourages us to examine them more closely. Table 6 shows how these multipliers perform with regard to lattice packing in the sample space

and in the dual space. A comparison of these results with those in Tables 2 and 3 makes clear that these multipliers are equally acceptable with regard to lattice packing considerations. Whether or not some other justifiable basis exists for choosing these multipliers over the best five is not apparent at present.

4. Empirical Evaluations

In addition to evaluating the global properties of a multiplier, one needs to consider the local randomness properties of subsequences of moderate length that a generator with this multiplier produces. This evaluation is usually performed by statistically testing these subsequences to detect departures from randomness. Fishman and Moore (1982) described a comprehensive battery of tests for this purpose, and we apply the same battery here to test the five best multipliers.

Recall from (2) that U_1, U_2, \dots are the random numbers normalized to $(0,1)$. Hypotheses to be tested include:

- H_0 : $\{U_i; i=1, \dots, n\}$ is a sequence of i.i.d. random variables.
- H_1 : $\{U_i; i=1, \dots, n\}$ have a uniform distribution on $(0,1)$.
- H_2 : (U_{2i-1}, U_{2i}) $i=1, \dots, n/2$ have a uniform distribution on the unit square.
- H_3 : $(U_{3i-2}, U_{3i-1}, U_{3i})$ $i=1, \dots, (n-2)/3$ have a uniform distribution on the unit cube.
- H_4 : H_0, H_1, H_2 and H_3 hold simultaneously.

For each multiplier we collected 100 consecutive subsequences of $n=200,000$ numbers. For each subsequence i and each hypothesis j a test statistic T_{ij} was computed. Then for hypothesis j , $T_{ij}, \dots, T_{100,j}$ were subjected to the battery of tests. Let T_{ij} have continuous cumulative distribution function (c.d.f.) G_j under hypothesis j . Then $G_j(T_{ij})$ and $P_{i,j} = 1 - G_j(T_{ij})$ are distributed uniformly on $(0,1)$ and for $0 < t < 1$

$$F_{n,j}(t) = \frac{1}{n} \sum_{i=1}^n I_{(0,t]}(P_{ij}),$$

where I_B denotes the indicator function on the set B , is an empirical c.d.f. If H_j is true

$$D_{n,j} = \sup_t |F_{n,j}(t) - t|$$

has the Kolmogorov-Smirnov (K-S) distribution,

$$V_{n,j} = n \int_0^1 I_{[0,t]}(F_{n,j}(t)) dt$$

has the uniform distribution on $(0,1)$ (Dwass 1958) and for large n

$$A_{n,j}^2 = n \int_0^1 \{[F_{n,j}(t) - t]^2 / t(1-t)\} dt$$

has a distribution given by Anderson and Darling (1952, 1954) and

is denoted by A-D. The quantity $D_{n,j}$ measures the absolute deviation between the empirical and the hypothesized c.d.f.;

$V_{n,j}$ measures the proportion of $F_{n,j}$ that lies below the

hypothesized c.d.f.; and $A_{n,j}^2$ is a weighted measure of the

extent of deviation, principally in the tails, of the empirical c.d.f.

Since Fishman and Moore (1982) provided complete descriptions of the testing of H_0, \dots, H_4 , here we merely review the most essential details. In particular each test statistic T_{ij} was chosen as follows. To test H_0 we relied on a comprehensive analysis of runs-up and runs-down statistics. For H_1 we chose a chi-squared goodness-of-fit statistic with $2^{12} = 4096$ cells. For H_2 the serial test statistic was used for nonoverlapping 2-tuples with a total of 4096 cells in the unit square. For H_3 , a serial test statistic was used for nonoverlapping 3-tuples and 4096 cells in the unit cube.

The hypothesis H_4 is omnibus in character. Recall that $P_{ij} = 1 - G_j(T_{ij})$ $i=1, \dots, 100$ $j=0, 1, \dots, 3$ and set

$$X_{ij} = \Phi^{-1}(P_{ij})$$

where Φ^{-1} is the inverse of the unit normal distribution.

Under H_j , X_{ij} has the unit normal distribution and X_{i0} ,

X_{i1}, \dots, X_{i3} have a multinormal distribution function ψ . Let

$X_{i,\min} = \min(X_{i,0}, \dots, X_{i,3})$ and $X_{i,\max} = \max(X_{i,0}, \dots, X_{i,3})$.

Then under H_4

$$\bar{T}_{i,4} = 1 - \psi(-X_{i,\min}, -X_{i,\min}, -X_{i,\min}, -X_{i,\min})$$

and

$$T_{i,4} = 1 - \psi(X_{i,\max}, X_{i,\max}, X_{i,\max}, X_{i,\max})$$

each have the unit normal distribution. Since $\bar{T}_{i,4}$ and $T_{i,4}$ measure how likely one is to encounter values as extreme as $X_{i,\min}$ and $X_{i,\max}$, they provide valuable information about the truth of

H_0, \dots, H_3 . Accordingly we used $\{\bar{T}_{i,4}; i=1, \dots, 100\}$ and $\{T_{i,4}; i=1, \dots, 100\}$ to test H_4 . As an interim result a test of the multinormality of $X_{i,0}, \dots, X_{i,3}$ was also performed.

Table 7 presents the P values for H_0, \dots, H_4 and the multinormality test for the five best multipliers. Although several multipliers show some small P values, no systematic rejection occurs across the K-S, V and A-D tests and across hypotheses. If one feels compelled to rank the multipliers, one might regard A=950706376 as first and A=1343714438 as last. However, we emphasize that in a table with so many entries some low values are to be expected when all hypotheses are true. In summary we conclude that, in addition to having optimal global properties, the five multipliers show no empirical aberrations.

References

- AHRENS, J. H. and U. DIETER (1977). Uniform Random Numbers, University of Graz.
- ANDERSON, T.W. and D.A. DARLING (1952). "Asymptotic Theory of Goodness of Fit Criteria Based on Stochastic Processes," Ann. Math. Statist., 23, 1983-212.
- ANDERSON, T.W. and D.A. DARLING (1954). "A Test of Goodness of Fit," J. Amer. Statist. Assoc., 49, 765-769.
- BEYER, W. A., R. B. ROOF and D. WILLIAMSON (1971). "The Lattice Structure of Multiplicative Congruential Pseudo-Random Vectors," Mathematics of Computation, 25, 345-363.
- BOROSH, S. and H. NIEDERREITER (1983). "Optimal Multipliers for Pseudo-random Number Generation by The Linear Congruential Method," Bit, 23, 65-74.
- CASSELS, J. W. S. (1959). An Introduction to the Geometry of Numbers, Springer-Verlag.
- COVEYOU R. R. (1970). "Random Number Generation is Too Important to be Left to Chance," Studies in Appl. Math., 3, 70-111.
- COVEYOU, R. R. and R. D. MacPHERSON (1967). "Fourier Analysis of Uniform Random Number Generators," J. Assoc. Comput. Mach., 14, 100-119.
- DWASS, M. (1958). "On Several Statistics Related to Empirical Distribution Functions," Ann. Math. Statist. 29, 188-191.
- DIETER, U. (1971). "Pseudo-random Numbers: The Exact Distribution of Pairs," Math. Comp., 25, 855-883.
- DIETER U. (1975). "How to Calculate Shortest Vectors in a Lattice," Mathematics of Computation, 29, 827-833.
- FISHMAN, G. S. and L. R. MOORE (1982). "A Statistical Evaluation of Multiplicative Congruential Random Number Generators with Modulus $2^{31}-1$," J. Amer. Statist. Assoc., 77, 129-136.
- HARDY, G. H. and E. M. WRIGHT (1960). The Theory of Numbers, 4th ed. Oxford: Clarendon Press.
- HOAGLIN D. (1976). "Theoretical Properties of Congruential Random-Number Generators: An Empirical View," Memorandum NS-340, Department of Statistics, Harvard University.

IMSL (1980). IMSL Library Reference Manual, Edition 8, IMSL INC., Houston Texas.

JANNSON, B. (1966). Random Number Generators, Stockholm: Almqvist and Wiksell.

KATZAN, H., JR. (1971). APL Users Guide, Van Nostrand Reinhold, New York.

KIVIAT, P., R. VILLANUEVA and H. MARKOWITZ (1969). The SIMSCRIPT II Programming Language, Prentice-Hall.

KNUTH, D. E. (1981). The Art of Computer Programming: Semi-numerical Algorithms, second ed., Addison-Wesley.

LEHMER, D. H. (1981). "Mathematical Methods in Large Scale Computing Units," Ann. Comp. Labs., Harvard University, 26, 141-146.

MARSAGLIA, G. (1968). "Random Numbers Fall Mainly in the Plane," Proc. Nat. Acad. Sci., 61, 25-28.

MARSAGLIA, G. (1972). "The Structure of Linear Congruential Sequences," in Applications of Number Theory to Numerical Analysis, ed. S. K. Zaremba, New York: Academic Press.

NEIDERREITER, H. (1976). "Statistical Independence of Linear Congruential Pseudo-random Numbers," Bull. Amer. Math. Soc., 82, 927-929.

NIEDERREITER, H. (1977). "Pseudo-random Numbers and Optimal Coefficients," Advances in Math. 26, 99-181.

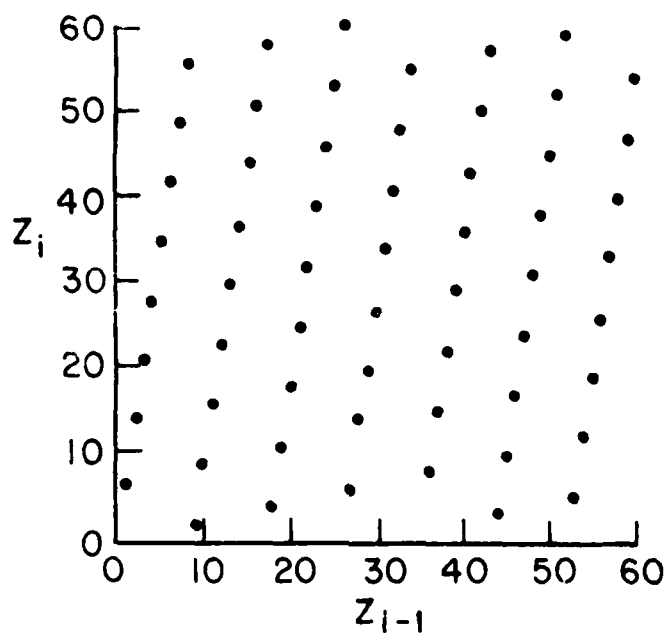
NEIDERREITER, H. (1978a). "The Serial Test for Linear Congruential Pseudo-random Numbers," Bull. Amer. Math. Soc. 84, 273-274.

NIEDERREITER, H. (1978b). "Quasi-Monte Carlo Methods and Pseudo-random Numbers," Bull. Amer. Math. Soc., 84, 957-1040.

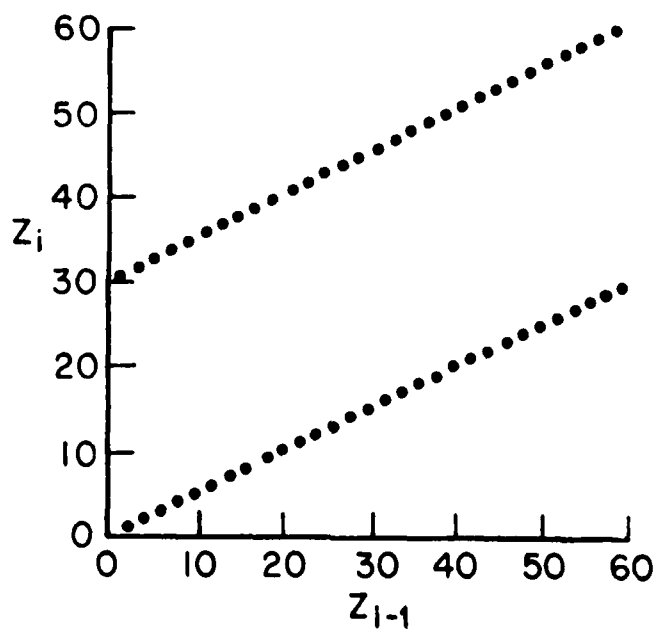
PAYNE, W. H., J. R. RABUNG and T. P. BOGYO (1969). "Coding the Lehmer Pseudorandom Number Generator," Comm. ACM, 12, 85-86.

SAS Institute Inc. (1982). SAS User's Guide: Basics, Cary, North Carolina.

SMITH, C. S. (1971). "Multiplicative Pseudo-Random Number Generators with Prime Modulus," J. ACM, 18, 586-593.



(a) $A = 7$



(b) $A = 31$

Fig. 1 $Z_i = AZ_{i-1} \pmod{6i}$

Table 1

Linear Congruential Generators: $Z_i \equiv AZ_{i-1} + C \pmod{M}$

Type	M	C	A	Z_0	Generated Sequence is a Permutation of	T
1	2^B	odd 1 mod 4		$\{0, 1, \dots, M-1\}$	$\{0, 1, \dots, M-1\}$	2^B
2	prime	0	primitive root of M	$\{1, \dots, M-1\}$	$\{1, \dots, M\}$	$M-1$
3a	2^B	0	5 (mod 8)	1 (mod 4)	$\{4j+1; j=0, 1, \dots, 2^{B-2}-1\}$	2^{B-2}
3b	2^B	0	5 (mod 8)	3 (mod 4)	$\{4j+3; j=0, 1, \dots, 2^{B-2}-1\}$	2^{B-2}
4a	2^B	0	3 (mod 8)	1 or 3 (mod 8)	$\{8j+1 \text{ and } 8j+3; j=0, 1, \dots, 2^{B-3}-1\}$	2^{B-2}
4b	2^B	0	3 (mod 8)	5 or 7 (mod 8)	$\{8j+5 \text{ and } 8j+7; j=0, 1, \dots, 2^{B-3}-1\}$	2^{B-2}

Source: Jannson (1966); A, C and Z_0 guarantee maximal period for the modulus $M=2^B$ with $B \geq 3$.

Table 2

Performance Measures for Selected Multipliers in $Z_i \equiv AZ_{i-1} \pmod{M}$ ^a

($M = 2^{31}-1$)

Multiplier		Dimension (k)				
A		2	3	4	5	6
742938285	S ₁	.8673	.8607	.8627	.8320	.8342
	S ₂	.8362	.6613	.6618	.6021	.6075
	S ₃	.8673	.8751	.8507	.7838	.7983
950706376	S ₁	.8574	.8985	.8692	.8337	.8274
	S ₂	.9211	.8183	.6555	.6806	.6822
	S ₃	.8574	.9093	.8412	.7565	.7646
1226874159	S ₁	.8411	.8787	.8255	.8378	.8441
	S ₂	.8273	.7240	.7815	.6492	.6822
	S ₃	.8411	.8877	.8468	.7107	.7743
62089911	S ₁	.8930	.8903	.8575	.8630	.8249
	S ₂	.7169	.7537	.7430	.7153	.6603
	S ₃	.8930	.8286	.7712	.8150	.7385
1343714438	S ₁	.8237	.8324	.8245	.8262	.8255
	S ₂	.8676	.6404	.6492	.6702	.7103
	S ₃	.8237	.7785	.7906	.7874	.7747
16807	S ₁	.3375	.4412	.5752	.7361	.6454
	S ₂	.2565	.3264	.5714	.6754	.5888
	S ₃	.3375	.5404	.6162	.6187	.5889
397204094	S ₁	.5564	.5748	.6674	.7678	.5947
	S ₂	.5966	.5038	.6239	.6597	.4206
	S ₃	.5564	.5543	.7302	.7849	.6417
630360016	S ₁	.8212	.4317	.7832	.8021	.5700
	S ₂	.8823	.4373	.6534	.7173	.5047
	S ₃	.8212	.6354	.6441	.7983	.5510
7	1000 S ₁	.1420	4.882	27.62	78.13	152.6
	1000 S ₂	.1221	3.413	16.81	41.19	74.77
	1000 S ₃	.1420	.02650	.02921	.06746	.2201

$$^a S_1 = \gamma_k / d_k^* (A, M) M^{1/k}, \quad S_2 = N_k^* (A, M) / (k! M)^{1/k} \text{ and } S_3 = c_k^* (A, M) \gamma_k M^{1/k}.$$

Table 3

Packing Measures in the Sample Space

$$\omega_k(A, M) = \pi^{k/2} M [c_k^*(A, M)]^k / \Gamma(k/2 + 1)$$

$$(M = 2^{31} - 1)$$

Dimension (k)

Multiplier A	2	3	4	5	6
742938285	2.73	3.97	5.17	4.40	6.17
950706376	2.67	4.45	4.94	3.69	4.77
1226874159	2.57	4.14	5.07	2.70	5.14
62089911	2.89	3.37	5.17	5.36	3.87
1343714438	2.46	2.80	3.86	4.51	5.16
16807	.41	.93	.00	1.35	1.00
397204094	1.12	1.01	2.80	4.44	1.67
630360016	2.45	1.52	1.70	4.83	.67
Upper Bound	3.63	5.92	9.87	14.89	23.87

Table 4
Parking Measures in the Dual Space

$$\mu_k(A, M) = \frac{\pi^{k/2}}{\Gamma(k/2+1) M[d_k^*(A, M)]^k} \\ (M=2^{31}-1)$$

Dimension (k)

Multiplier A	2	3	4	5	6
742938285	2.73	3.78	5.47	5.94	8.04
950706376	2.67	4.30	5.63	6.00	7.66
1226874159	2.57	4.02	4.58	6.15	8.63
62089911	2.14	4.34	4.23	4.77	7.99
1343714438	2.46	3.42	4.56	5.73	7.55
16807	.41	.51	1.08	3.22	1.73
397204094	1.12	1.13	1.96	3.97	1.06
630360016	2.45	.48	3.71	4.94	.82
Upper Bound	3.63	5.92	9.87	14.89	23.87

Table 5
Bounds on Discrepancy

Multiplier		Dimension (k)				
A		2	3	4	5	6
742938285	Lower ^a Upper ^b	.1492 3.446	.5970	42.89	42.89	42.89
950706376	Lower Upper	.2680 3.725	1.072	9.607	10.08	10.08
1226874159	Lower Upper	1.967 10.52	7.869	7.869	7.869	14.86
62089911	Lower Upper	.4236 6.333	1.694	1.694	1.694	4.328
1343714438	Lower Upper	.2541 3.772	1.016	1.016	1.016	7.045
16807	Lower Upper	1488 5952	5950	5950	5950	5950
397204094	Lower Upper	.4256 4.517	1.702	1.702	1.702	28.61
630360016	Lower Upper	.1502 2.980	.6008	1.546	1.546	4.057
7	Lower Upper	3571400 14286000	14286000	14286000	14286000	14286000

$$^a \text{Lower Bound} = 10^8 \times 1/\min (\lambda_{\pi} \prod_{i=0}^{k-1} |q_i|).$$

$$^b \text{Upper Bound} = 10^8 \times (2 + \sum_{i=1}^p a_i)/T.$$

Table 6

Packing Measures for Multipliers with
 $S_{1,k}(A,M) \geq .8$ and $S_{3,k}(A,M) \geq .8$ $k=2, \dots, 6$

Multiplier		Dimension (k)				
A		2	3	4	5	6
809609776	$\omega_k(A,M)$	3.17	3.76	4.51	4.51	8.26
	$\mu_k(A,M)$	3.17	4.23	4.55	5.07	6.71
1567699476	$\omega_k(A,M)$	2.88	3.66	4.98	6.55	9.96
	$\mu_k(A,M)$	2.88	3.15	4.37	5.72	6.71
1294711786	$\omega_k(A,M)$	3.08	2.72	4.95	5.44	9.85
	$\mu_k(A,M)$	3.08	4.73	4.73	4.17	5.65
1554283637	$\omega_k(A,M)$	2.56	3.71	4.71	6.08	7.79
	$\mu_k(A,M)$	2.56	4.15	4.27	5.74	6.38
857010188	$\omega_k(A,M)$	2.39	4.16	5.97	5.21	7.74
	$\mu_k(A,M)$	2.39	4.20	6.39	5.95	5.08
1582405117	$\omega_k(A,M)$	3.09	3.13	4.02	4.85	8.02
	$\mu_k(A,M)$	3.09	4.25	5.24	4.88	5.78
Upper Bound		3.63	5.92	9.87	14.89	23.87

Table 7

P Values for Testing Hypotheses

Multiplier A	Test (1)	H ₀ (2)	H ₁ (3)	H ₂ (4)	H ₃ (5)	Multi- normality (6)	H ₄	
							min (7)	max (8)
742938285	K-S	.735	.499	.306	.633	.922	.776	.802
	V	.853	.012 ^b	.971	.491	.463	.278	.353
	A-D	.408	.231	.406	.796	.990	.545	.870
950706376	K-S	.361	.304	.636	.766	.163	.244	.529
	V	.974	.827	.616	.493	.443	.401	.322
	A-D	.269	.254	.497	.629	.173	.279	.417
1226874159	K-S	.738	.115	.081 ^a	.903	.151	.220	.532
	V	.378	.468	.646	.395	.183	.425	.749
	A-D	.442	.083 ^a	.172	.914	.166	.420	.802
62089911	K-S	.232	.506	.493	.073 ^a	.578	.121	.132
	V	.618	.923	.773	.193	.160	.305	.345
	A-D	.328	.457	.539	.139	.377	.151	.144
1343714438	K-S	.771	.068 ^a	.024 ^b	.845	.635	.904	.230
	V	.849	.440	.158	.781	.577	.365	.404
	A-D	.806	.099 ^a	.041 ^b	.863	.542	.903	.195

^a.05 < P Value ≤ 0.1.

^b.01 < P Value ≤ .05.

^cP Value ≤ .01.

Appendix[†]

A	min $S_{1,k}$ k	min $S_{3,k}$ k	A	min $S_{1,k}$ k	min $S_{3,k}$ k
742938285	0.8319	0.7838	1700624889	0.8112	0.7943
950706376	0.8274	0.7565	1442273554	0.8111	0.7110
1226874159	0.8255	0.7107	959387418	0.8110	0.7790
62089911	0.8249	0.7385	1113127164	0.8108	0.7726
1343714438	0.8236	0.7747	1446285050	0.8107	0.7677
2049513912	0.8232	0.6545	231487336	0.8107	0.7820
781259587	0.8212	0.7699	231487336	0.8107	0.7820
482926380	0.8204	0.7489	403636263	0.8102	0.7946
1810831696	0.8198	0.7652	365370474	0.8098	0.7375
502005751	0.8196	0.6930	1683348964	0.8098	0.7113
484822633	0.8191	0.7366	56469953	0.8095	0.7021
1980369868	0.8186	0.7345	391539536	0.8095	0.7495
329440414	0.8184	0.7271	621589603	0.8093	0.7676
1930251322	0.8182	0.7199	1697336722	0.8092	0.7616
800218253	0.8182	0.7386	209720443	0.8092	0.7582
1575965843	0.8181	0.7242	1651132469	0.8090	0.7805
1106494401	0.8170	0.6826	1036489797	0.8090	0.7381
1647274979	0.8168	0.7124	1094002855	0.8086	0.7044
62292588	0.8166	0.7594	958373200	0.8088	0.7173
1904565529	0.8166	0.7577	1882462218	0.8087	0.7956
1032193948	0.8164	0.7470	1901918329	0.8087	0.7586
1734050460	0.8155	0.7455	1482800924	0.8084	0.7763
1580650638	0.8154	0.7723	1609286051	0.8079	0.7430
1622264322	0.8154	0.7076	1873448661	0.8075	0.6724
30010801	0.8152	0.7441	1394633840	0.8075	0.7039
1187848453	0.8150	0.7312	1691916501	0.8075	0.7119
531759225	0.8148	0.7179	155279822	0.8075	0.6776
1402531614	0.8147	0.7277	1499553667	0.8073	0.7992
928795757	0.8145	0.7567	2117506721	0.8073	0.7198
1667403910	0.8144	0.7545	1337239139	0.8072	0.7897
1434972591	0.8142	0.7517	1257761541	0.8072	0.7358
1542873971	0.8142	0.7938	1061023796	0.8072	0.7087
621506530	0.8141	0.7158	659947220	0.8071	0.6689
473911476	0.8139	0.7548	1472802766	0.8071	0.7432
2110382506	0.8139	0.7783	1709354462	0.8069	0.7457
150663646	0.8138	0.7012	1437555212	0.8069	0.7240
131698448	0.8136	0.7740	2112159807	0.8069	0.7122
1114950053	0.8133	0.7568	1610356818	0.8068	0.7029
1768650394	0.8130	0.7509	1362325644	0.8066	0.6909
513482567	0.8127	0.7803	1528100652	0.8066	0.7778
513482567	0.8127	0.7803	644912347	0.8067	0.7856
1626240045	0.8127	0.7308	1640011312	0.8063	0.7232
2099489754	0.8127	0.7468	1267261170	0.8062	0.7771
1262413818	0.8127	0.6294	809609776	0.8061	0.8222
334633198	0.8125	0.6849	292357876	0.8061	0.7322
404208769	0.8124	0.7266	1022131410	0.8061	0.7509
572960339	0.8124	0.7366	1636624282	0.8061	0.7595
1606074663	0.8121	0.7780	672536717	0.8060	0.7532
1393492757	0.8121	0.7484	1292868646	0.8059	0.6673
464026286	0.8115	0.7029	965146404	0.8059	0.7546

[†]The remaining 207 multipliers can be computed as follows: Set $B = 7$;
for each multiplier A find the smallest integer I such that $A \equiv B^I \pmod{M}$.
Then the multiplier $A^* \equiv B^{M-1-I} \pmod{M}$ has the same properties as A .

Appendix (continued)

A	min $S_{1,k}$ k	min $S_{3,k}$ k	A	min $S_{1,k}$ k	min $S_{3,k}$ k
1493834601	0.8059	0.6905	737154017	0.8023	0.7564
1037566960	0.8058	0.7469	764376606	0.8023	0.6581
743722486	0.8058	0.7659	1074109599	0.8023	0.7944
1509089437	0.8057	0.7264	1039215247	0.8023	0.6029
1567699476	0.8057	0.8426	426641844	0.8022	0.6706
1947306937	0.8053	0.7164	1522856686	0.8022	0.7635
1076532097	0.8052	0.7503	1019054714	0.8020	0.7589
1957811727	0.8052	0.6339	805874727	0.8019	0.7295
628467148	0.8051	0.7540	1165699491	0.8018	0.7391
1049695393	0.8049	0.7252	258886375	0.8017	0.7245
786824435	0.8049	0.7905	1554283637	0.8017	0.8094
556530824	0.8049	0.7320	1155862579	0.8017	0.7911
87911290	0.8047	0.7402	643376760	0.8016	0.5756
1457913431	0.8047	0.7966	915892507	0.8016	0.7204
385787459	0.8046	0.7596	614775685	0.8016	0.7329
1567316532	0.8046	0.7566	391842496	0.8015	0.7255
930959341	0.8044	0.7796	380006810	0.8015	0.7456
1588813465	0.8044	0.7850	2011769251	0.8014	0.6802
1035519219	0.8043	0.7590	1860139263	0.8014	0.7729
36944245	0.8043	0.6932	1920577088	0.8014	0.6861
1891356973	0.8043	0.7058	1993412958	0.8014	0.7026
1897412292	0.8043	0.7112	511806823	0.8014	0.6100
754666739	0.8043	0.7447	979167897	0.8014	0.7860
1971204812	0.8043	0.7753	1956806422	0.8012	0.7521
1888847798	0.8042	0.6658	1256909708	0.8011	0.6410
1571641634	0.8040	0.7445	581488682	0.8011	0.6365
1117435554	0.8040	0.7243	334258581	0.8011	0.7065
569170662	0.8040	0.7292	68580478	0.8011	0.7568
927407259	0.8040	0.7149	534897944	0.8011	0.7808
1490690267	0.8039	0.7250	251676340	0.8009	0.6418
235716977	0.8039	0.7313	1051072528	0.8009	0.7125
149289625	0.8038	0.7026	2101655234	0.8009	0.7710
1666576129	0.8038	0.7851	1413698051	0.8008	0.7819
1517266157	0.8038	0.6327	796322341	0.8008	0.7611
1229681012	0.8037	0.7146	698106846	0.8008	0.7543
707656279	0.8037	0.7617	1544249456	0.8008	0.7187
1869095734	0.8037	0.6714	857010168	0.8008	0.8001
995560464	0.8037	0.7182	1860498201	0.8008	0.7639
539146268	0.8037	0.7505	35389105	0.8008	0.6647
1604167179	0.8036	0.7013	1774722449	0.8007	0.7413
2082150220	0.8035	0.7624	1582405117	0.8007	0.8176
370594724	0.8035	0.7375	553469741	0.8007	0.7233
2044924591	0.8035	0.6988	1411007767	0.8006	0.6678
916100787	0.8035	0.6079	1230102545	0.8006	0.7507
1037414126	0.8035	0.7866	356267478	0.8005	0.7199
1336122410	0.8033	0.7246	778084663	0.8005	0.7903
1265438464	0.8031	0.6262	1905014417	0.8005	0.6762
1007804709	0.8029	0.6410	1109871330	0.8005	0.7312
1257431879	0.8029	0.7676	1704316220	0.8004	0.7326
2061749697	0.8029	0.6603	270593738	0.8004	0.6510
737009774	0.8026	0.7135	483389111	0.8003	0.7821
408432740	0.8024	0.7514	323128013	0.8003	0.7395
876389446	0.8024	0.7398	361076890	0.8000	0.7293
1294711786	0.8024	0.8040			

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM	
1. REPORT NUMBER UNC/ORSA/TR-84/5	GOVT ACCESSION NO. AD-A143085	3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle) AN EXHAUSTIVE ANALYSIS OF MULTIPLICATIVE CONGRUENTIAL RANDOM NUMBER GENERATORS WITH MODULUS $2^{31}-1$	5. TYPE OF REPORT & PERIOD COVERED TECHNICAL REPORT		
	6. PERFORMING ORG. REPORT NUMBER		
7. AUTHOR(s) GEORGE S. FISHMAN and LOUIS R. MOORE III	8. CONTRACT OR GRANT NUMBER(s) C N00014-76-0302		
9. PERFORMING ORGANIZATION NAME AND ADDRESS CURRIC. IN OPERATIONS RESEARCH & SYSTEMS ANALYSIS SMITH BUILDING 128A UNIV. OF NORTH CAROLINA CHAPEL HILL, NC 27514	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS		
11. CONTROLLING OFFICE NAME AND ADDRESS NAVAL ANALYSIS PROGRAM OFFICE OF NAVAL RESEARCH ARLINGTON, VA 22217	12. REPORT DATE June 1984		
	13. NUMBER OF PAGES 44		
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)	15. SECURITY CLASS. (of this report)		
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE		
16. DISTRIBUTION STATEMENT (of this Report) DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED.			
<div style="border: 1px solid black; padding: 5px; text-align: center;"> DISTRIBUTION STATEMENT A Approved for public release Distribution Unlimited </div>			
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report) UNCLASSIFIED			
18. SUPPLEMENTARY NOTES			
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) CONGRUENTIAL GENERATOR, DISCREPANCY, LATTICE TEST, RANDOM NUMBER GENERATION, SPECTRAL TEST.			
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) This paper presents the results of an exhaustive search to find optimal full period multipliers for the multiplicative congruential random number generator with prime modulus $2^{31}-1$. Here a multiplier is said to be optimal if the distance between adjacent parallel hyperplanes on which k-tuples lie			

does not exceed the minimal achievable distance by more than 25 percent for $k=2, \dots, 6$. This criterion is considerably more stringent than prevailing standards of acceptability and leads to a total of only 414 multipliers among the more than 534 million candidate multipliers.

Section 1 reviews the basic properties of linear congruential generators and Section 2 describes worst case performance measures. These include the maximal distance between adjacent parallel hyperplanes, the minimal number of parallel hyperplanes, the minimal distance between k -tuples, the lattice ratio and the discrepancy. Section 3 presents the five best multipliers and compares their performances with those of three commonly employed multipliers for all measures but the lattice test. Comparisons using packing measures in the space of k -tuples and in the dual space are also made. Section 4 presents the results of applying a battery of statistical tests to the best five to detect local departures from randomness. None were found. The Appendix contains a list of all optimal multipliers.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

ATE
LME